1215418

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

August 22, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/482,628*
FILING DATE: *June 25, 2003*
RELATED PCT APPLICATION NUMBER: *PCT/US04/20562*

Certified by

Jon W Dudas

Acting Under Secretary of Commerce
for Intellectual Property
and Acting Director of the U.S.
Patent and Trademark Office

PTO/SB/16 (10-01)
Approved for use through10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No.	EU245163295US

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Lance M.	Cottrell	San Diego, California
James A	Reynolds	Carlsbad, California
Darya	Mazandarany	San Diego, California

☑ *Additional inventors are being named on the* 1 *separately numbered sheets attached hereto*

11507 U.S. PTO
06/25/03

TITLE OF THE INVENTION (500 characters max)

A SECURE NETWORK PRIVACY SYSTEM

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☐ Customer Number _____ → *Place Customer Number Bar Code Label here*

OR *Type Customer Number here*

☑ Firm or Individual Name	Francisco A. Rubio-Campos				
Address	The Eclipse Group				
Address	26895 Aliso Creek Road, Suite B-104				
City	Aliso Viejo	State	CA	ZIP	92656
Country	USA	Telephone	949-448-9410	Fax	714-948-8903

ENCLOSED APPLICATION PARTS *(check all that apply)*

☑ Specification *Number of Pages* 12
☑ Drawing(s) *Number of Sheets* 4
☐ Application Data Sheet. See 37 CFR 1.76
☐ CD(s), Number
☐ Other (specify)

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.
☑ A check or money order is enclosed to cover the filing fees
☑ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 502542
☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($): $80.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☑ No.
☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE _____ Date 06/25/2003

TYPED or PRINTED NAME Francisco A. Rubio-Campos

REGISTRATION NO. *(if appropriate)* 45,358

TELEPHONE (949) 448-9410

Docket Number: ~~IF0300USV~~ IF0300 3USV

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

PTO/SB/17 (05-03)
Approved for use through 04/30/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 80.00

Complete if Known	
Application Number	Unknown
Filing Date	June 25, 2003
First Named Inventor	Lance M. Cottrell et al.
Examiner Name	Not applicable
Art Unit	Unassigned
Attorney Docket No.	IF03003USV

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☑ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 502542

Deposit Account Name: The Eclipse Group

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☐ Charge any additional fee(s) during the pendency of this application

☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	750	2001	375	Utility filing fee	
1002	330	2002	165	Design filing fee	
1003	520	2003	260	Plant filing fee	
1004	750	2004	375	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	80.00

SUBTOTAL (1) ($) 80.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below	Fee Paid
Total Claims	-20** =	X		=
Independent Claims	- 3** =	X		=
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	84	2201	42	Independent claims in excess of 3
1203	280	2203	140	Multiple dependent claim, if not paid
1204	84	2204	42	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	410	2252	205	Extension for reply within second month	
1253	930	2253	465	Extension for reply within third month	
1254	1,450	2254	725	Extension for reply within fourth month	
1255	1,970	2255	985	Extension for reply within fifth month	
1401	320	2401	160	Notice of Appeal	
1402	320	2402	160	Filing a brief in support of an appeal	
1403	280	2403	140	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,300	2453	650	Petition to revive - unintentional	
1501	1,300	2501	650	Utility issue fee (or reissue)	
1502	470	2502	235	Design issue fee	
1503	630	2503	315	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	750	2809	375	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	750	2810	375	For each additional invention to be examined (37 CFR 1.129(b))	
1801	750	2801	375	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0.00

SUBMITTED BY

Name (Print/Type)	Francisco A. Rubio-Campos	Registration No. (Attorney/Agent)	45,358	(Complete *if applicable*) Telephone	949-448-9410
Signature				Date	June 25, 2003

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PROVISIONAL APPLICATION COVER SHEET
Additional Page

PTO/SB/16 (02-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Docket Number	IF03003USV

INVENTOR(S)/APPLICANT(S)

Given Name (first and middle [if any])	Family or Surname	Residence (City and either State or Foreign Country)
Steve	Walsh	Tara QLD 4421, Australia
Peleus	Uhley	Alameda, California
Gene	Nelson	Spring Valley, California

Number 2 of 2

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

U.S. Express Mail No.: EU245163295US
Filing Date: June 25, 2003

PATENT
Docket No. IF03003USV

A SECURE NETWORK PRIVACY SYSTEM

INVENTORS

LANCE M. COTTRELL
JAMES A REYNOLDS
DARYA MAZANDARANY
STEVE WALSH
PELEUS UHLEY
&
GENE NELSON

BACKGROUND OF THE INVENTION

[001] **1. Field of the Invention.**

[002] This invention relates generally to network communication systems. In particular, this invention relates to an Internet privacy system capable of operating across multiple platforms.

[003] **2. Related Art.**

[004] As the global computer network known as the Internet continues to grow globally at a rapid pace, an increasing number of people and businesses from around the world are accessing the Internet for both business and personal activities. As a result, the Internet has become a virtual community were people communicate with each other by sending and receiving electronic, voice and image messages for business and pleasure. These communications include sharing ideas and information, sending personal and business message back and forth, researching information, expressing opinions and ideas both personal and political, and conducting business negotiations and transactions (generally known as "electronic commerce" or "e-commerce"). In response to this new

electronic activity, business, governments and certain individuals attempt to identify and track individual Internet users for numerous purposes including, but not limited to, advertising, market research, customizing information of Internet sites (i.e., "websites") snooping and ease dropping on communications, political and law enforcement activities, fraud and malicious activities. Many of these attempts are threats to the individual users of the Internet because they attempt to gain personal information about the user and the user's activities on the Internet (generally referred to as the user's "online activities") typically without the user's express consent or knowledge.

[005] These threats typically gain information about the user by logging a user's Internet Protocol ("IP") address (the electronic address that specifically identifies a user's computer to the network) or by installing programs or files on to the user's computer such as "cookies," ActiveX™ applications, Java™, script files, Spyware, or hostile programs such as viruses. These threats allow an outside user, be it a government, business, or individual entity, to perform such tasks as identify a user, obtaining the user's personal information that is stored on the computer (including names, address, financial, private files, and/or other confidential, private and/or sensitive information), and track the user's activities on the Internet including recording every website visited or every email sent or received by the user. Malicious programs such as viruses may also be installed on the user's computer that can modify, erase or destroy the user's operating system of personal files.

[006] Unfortunately, most people that utilize the Internet do not understand technically how networks such as the Internet function nor do they generally appreciate

the number and types of threats that they will experience once they connect (i.e., "log-on") to the Internet. Past attempts at protecting users on the internet include using "firewalls" to block certain types of threats from the Internet, virus protection programs for detecting malicious programs, and spyware and cookie file removal software. However, these past attempts do not protect a user's identity because most of these approaches attempt to disinfect a user from intruders after the fact. These past approaches do not protect a user's identity as soon as the user connects to the Internet because connected websites are able to read and identify the user's IP address among other things. A need therefore exist to protect a user's identity as soon as the user connects to the Internet (i.e., known as "surfing the web" or "surfing the Net").

[007] Attempts in the past at protecting the user's identity have included allowing a user to connect to an intermediate server connected to the Internet that extracted off the user's IP information and substituted it with the IP address of the intermediate server thus creating an anonymous user that could then continue to surf the Net without worrying that their IP information would be used to identify them.

[008] Unfortunately, this approach was too technical and difficult to operate by most Internet users. Therefore, there is a need for a privacy management system that solves the problems recited above and allows Internet users to easily maintain their privacy by utilizing an anonymous server.

BRIEF DESCRIPTION OF THE FIGURES

[009] The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views.

[010] FIG. 1 shows a signal flow diagram of an example process for HTTP request with full time SSL on.

[011] FIG. 2 shows a signal flow diagram of an example process for requests made using SSL.

[012] FIG. 3 shows a flow chart for an example process performed by the architecture of the invention.

[013] FIG. 4 shows a signal flow diagram of an example process for determining the sequence of events on a client proxy.

DETAILED DESCRIPTION

[014] This invention describes a method for providing Internet privacy service which shall be described in relation to example implementation herein referred to as AnonPro. AnonPro may be a specific implementation of our inventions for providing Internet privacy services. The components described in this detailed description and figures are an example implementation for some of our particular applications, however, the technologies and inventions described herein are much more general. The components are generally a network level traffic interceptor (client side), a client proxy, a server proxy, an SSL module, and some web based services (such as the user

authentication, server lists, recommended site settings lists etc.). Generically speaking, the combination of the components is an "Internet privacy system." The client part is "Internet Privacy Client", while the server proxy is "Internet Privacy remote proxy." In the description of this invention we often refer to registry entries or other specific ways of storing information. In all cases this information could be stored in any number of ways including in flat files, indexed files, local or remote databases, among others. In the description of this invention we often refer to cookies. Many other information transfer techniques could be used in place of cookies including HTML headers, changes to URLs or other addresses, any other standard or custom message or data structure. In the description of this invention we often refer to XML data structures. In general these structures could be replaced with any other kind of data structure, including other standard and non-standard, encrypted and non-encrypted structures. CA stands for "Certificate Authority" and refers to an entity or encryption key used for signing other keys such as SSL keys.

[015] Additionally, The AnonPro Server Proxy (also known as the "Internet Privacy Remote Proxy") is a system that relays data from the client on the user's PC to the computer hosting the content or service the user is trying to access through the system's Internet Privacy System (the Destination). The proxy acts to hide the user's IP address and may perform other actions based on the content of the request or the contents of the reply from the Destination. These actions may include adding, changing, or removing text, data, information, scripts or other content from either the data from the user to the destination, or from the destination back to the user. The Internet Privacy Remote Proxy

is not used in all modes of the Internet Privacy Client. In some modes the Internet Privacy Client connects directly to the Destination. Whether or not the Internet Privacy Remote Proxy is used depends on the privacy settings the user has set for that particular site. The Internet Privacy Remote Proxy is only used if the hiding of the user's IP, or the other changes the Remote Proxy makes to the data, are required for the particular settings. Otherwise the connection is direct.

[016] This invention to provides SSL functionality for the AnonPro client. Full time SSL will enable users of the client to connect securely to the proxy if they are using any of the http protocols such as http://www.yahoo.com or https://www.yahoo.com. This invention benefits a user in at least two ways. First, a user is able to receive a secure means of communication with our proxy so that we don't introduce any more threats. Second, we effectively implement a man in the middle attack allowing us to seamlessly filter the users content for them even if they are browsing secure sites.

[017] The client code may provide hooks to redirect traffic to the client side Proxy Server (that will be described below). That server may be a fully functional web proxy that may process the https connection using the SSL module. The SSL module may be called by the client proxy server when it receives an https connection. This may happen in two ways described in FIG. 1 and FIG. 2. The first way is described by FIG. 1 that shows a signal flow diagram of an example process for HTTP request with full time SSL on. The second way is described by FIG. 2 that shows a signal flow diagram of an example process for requests made using SSL.

[018] In terms of Architecture, the Client hooks module may be a placeholder for calls and callbacks but the Client Proxy Server may be a fully functional server. This means that it may listen on ports for incoming secure as well as insecure connections and possibly spawning a new thread to handle each connection. When the client is installed the User CA keys should be generated, also the Public User CA key may be installed in the browser automatically but if this isn't possible we may provide instructions on how to do it manually. A universal site key may be utilized that may be signed by the User's Secret CA key to forge the authentication of the secure site. For security reasons, a background thread may be spawned on startup to generate a new key and swap with the universal site key after it has been generated. The universal site key may be generated and stored in many ways and at many times. For example, it could be changed for every site, or reused for every site.

[019] FIG. 3 shows a flow chart for an example process performed by the architecture of the invention, which shows how the identity of the secure server the browser wishes to connect to is assumed. In FIG. 3, when a request comes in for a secure site the system may check to see if the system has the site cert to return in the SSL handshake. To store the certificates the system may use a SHA-1 hash of the server they are representing. If the system cannot find the certificate in the system's cache the system will generate one for that site using the system's universal site certificate and the User CA Secret Key. Once generated this is stored in the cache.

[020] After all of the above is completed the system may finish the SSL handshake and begin the man in the middle attack. Essentially what the system is doing is decoding

the SSL records on the client proxy server redirecting them through the filtering code and then doing an SSL_Write to the anonymizer proxy or directly to the destination web site. A similar flow is used when reading data from the anonymizer proxy where the system does an SSL_Read giving the system the clear text that was sent. Then the system sends it though the filtering code. Finally the system may do an SSL_Write to the client, which will return it to the browser.

[021] FIG. 4 shows a signal flow diagram of an example process for determining the sequence of events on a client proxy. In FIG. 4, the sequence of events on the Client proxy may be as follows. The TCP hook has redirected the browser request to the system, the system then calls the regular socket accept and makes a call to SSL_Initialize. The client proxy SSL handler may then make calls to SSL_read/write instead of the standard recv and send calls.

[022] It is appreciated that the Client Proxy server should be very reliable so as not to have multiple servers listening on the same port because the system should not have more than one on each client. In order to prevent vulnerabilities in the system the server should do some form of client authentication to make sure other applications or even machines are trying to use the client proxy server.

[023] The processes described in FIG. 1 through FIG. 4 may be performed by hardware or software. If the process is performed by software, the software may reside in software memory (not shown) in the controller, memory, or an removable memory medium. The software in memory may include an ordered listing of executable instructions for implementing logical functions (i.e., "logic" that may be implement either

in digital form such as digital circuitry or source code or in analog form such as analog circuitry or an analog source such an analog electrical, sound or video signal), may selectively be embodied in any computer-readable (or signal-bearing) medium for use by or in connection with an instruction execution system, apparatus, or device, such as a computer-based system, processor-containing system, or other system that may selectively fetch the instructions from the instruction execution system, apparatus, or device and execute the instructions. In the context of this document, a "computer-readable medium" and/or "signal-bearing medium" is any means that may contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The computer readable medium may selectively be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific examples "a non-exhaustive list" of the computer-readable medium would include the following: an electrical connection "electronic" having one or more wires, a portable computer diskette (magnetic), a RAM (electronic), a read-only memory "ROM" (electronic), an erasable programmable read-only memory (EPROM or Flash memory) (electronic), an optical fiber (optical), and a portable compact disc read-only memory "CDROM" (optical). Note that the computer-readable medium may even be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via for instance optical scanning of the paper or other medium, then compiled, interpreted or otherwise processed in a suitable manner if necessary, and then stored in a computer memory.

[024] In general, the system described provides for Consensual Man in the Middle Attack by using used to rewrite pages, on the fly creation of site SSL certificates, CA cert to sign all SSL site certificates, CA cert is generated per user, CA cert is automatically installed in the browser and SSL page rewriting. Where the SSL page rewriting included the Client decrypting SSL pages to rewrite before re-encrypting and sending to proxy or end web site.

[025] The system also provides for the Client to Insert information into data stream from browser to Internet through any kind of Header or by inserting cookies. The cookies may include authentication / access rights information and preferences information and utilize XML and encryption.

[026] The system may also provides for a TCP level hook for privacy service that includes the Hook redirecting traffic to a local proxy on the user's machine, the Client proxy redirecting traffic to Anonymizer proxy and the TCP hook allows IP hiding.

[027] The system may also provides for a Full time SSL without URL prefixing.

[028] The system may also provides for making cookies session only and/or change cookie expiration date.

[029] The system may also provides for gathering and generation Privacy Statistics that include Per site privacy statistics, a Privacy Analyzer real time threat display, and automated site threat analysis and rating.

[030] The system may also provides for setting per site privacy settings that include white lists, black lists, detailed custom settings, "Show details" functionality, recommended site settings list that include automatically updated and downloaded

settings, and hard coded Site settings that can't be changed by user have preset defaults and an exception list for some sites.

[031] The system may also provides for the Client to keep a list of alternate access names / IP addresses for accessing servers. The Client may tries all addresses one after another and/or each user gets a different set of access addresses.

[032] The system may also provides allows install on many computers while detect and prevent multiple simultaneous users.

[033] The system may also provides allows Client Javascript [script] rewriting. The system utilizes a novel GUI design to manage information.

[034] While various embodiments of the application have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible that are within the scope of this invention. Accordingly, the invention is not to be restricted except in light of the attached claims and their equivalents. The foregoing description of an implementation has been presented for purposes of illustration and description. It is not exhaustive and does not limit the claimed inventions to the precise form disclosed. Modifications and variations are possible in light of the above description or may be acquired from practicing the invention. For example, the described implementation includes software but the invention may be implemented as a combination of hardware and software or in hardware alone. Note also that the implementation may vary between systems. The claims and their equivalents define the scope of the invention.

CLAIMS

What is claimed is:

1. A method for allowing a user to connect to a privacy network comprising:

connecting to the network;

receiving a user name and password from a user; and

determining whether the user account is valid.

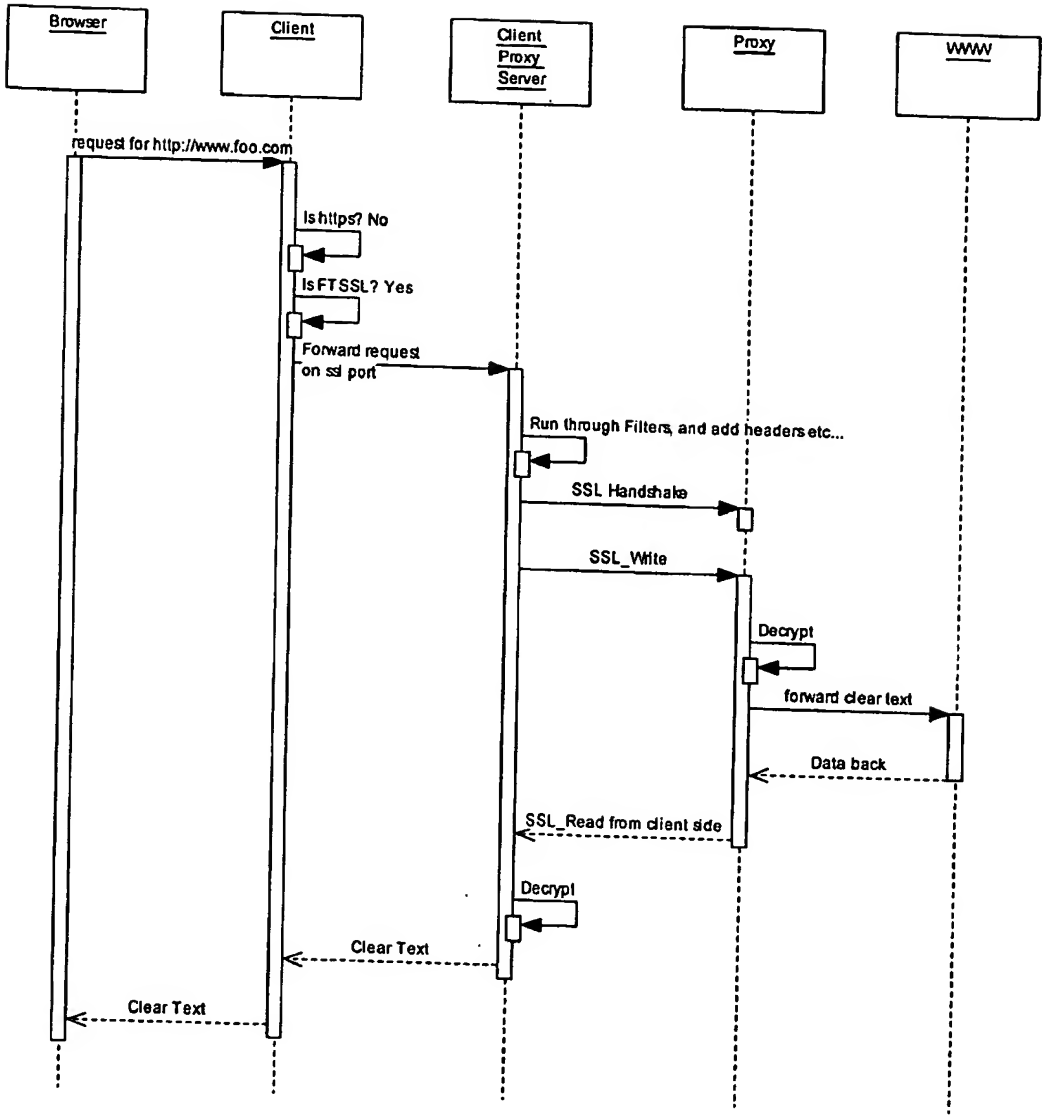
Browser
Client
Client Proxy Server
Proxy
WWW
request for http://www.foo.com
Is https? No
Is FTSSL? Yes
Forward request on ssl port
Run through Filters, and add headers etc...
SSL Handshake
SSL_Write
Decrypt
forward clear text
Data back
SSL_Read from client side
Decrypt
Clear Text
Clear Text

FIG. 1

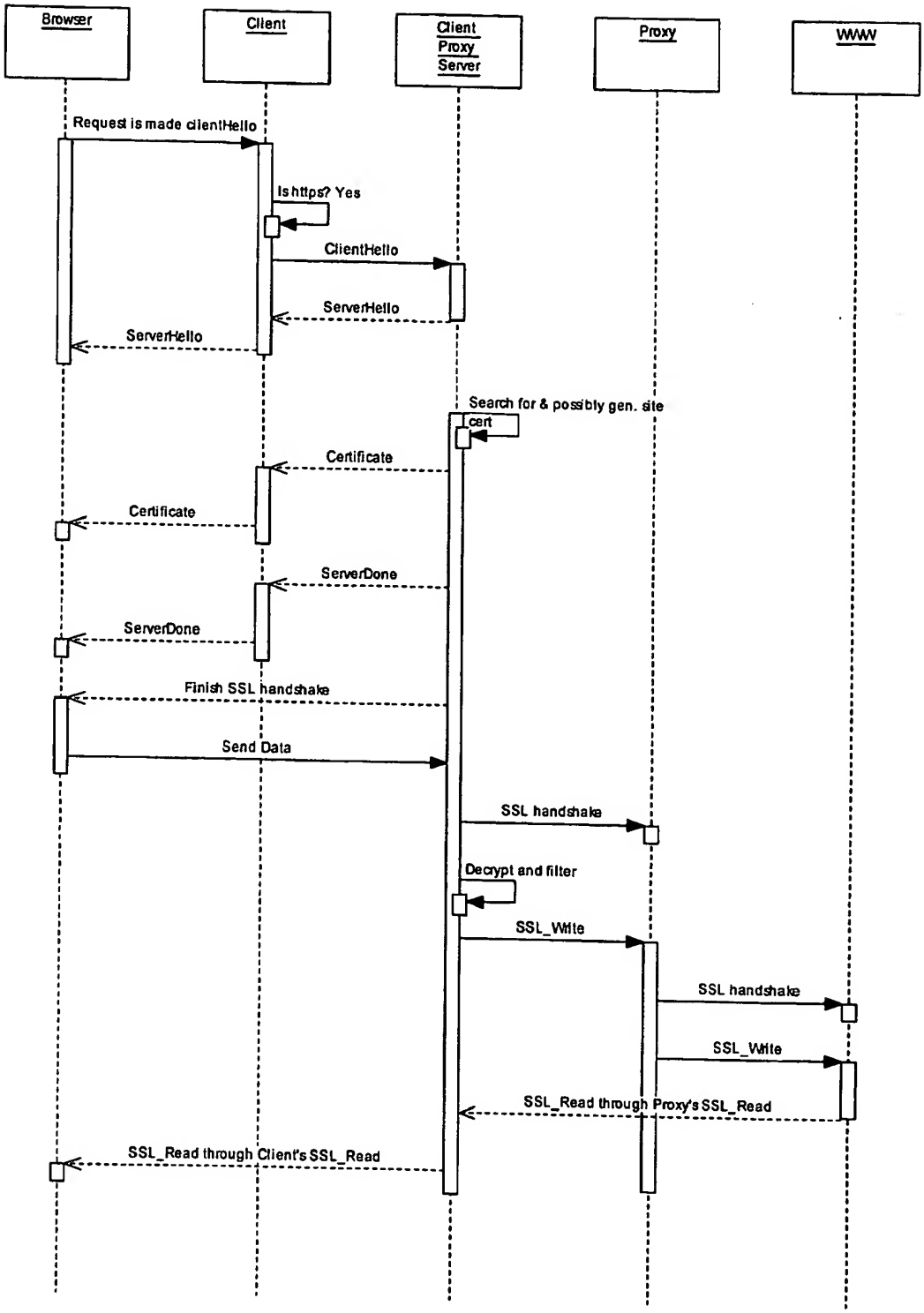
Browser
Client
Client Proxy Server
Proxy
WWW
Request is made clientHello
Is https? Yes
ClientHello
ServerHello
ServerHello
Search for & possibly gen. site cert
Certificate
Certificate
ServerDone
ServerDone
Finish SSL handshake
Send Data
SSL handshake
Decrypt and filter
SSL_Write
SSL handshake
SSL_Write
SSL_Read through Proxy's SSL_Read
SSL_Read through Client's SSL_Read

FIG. 2

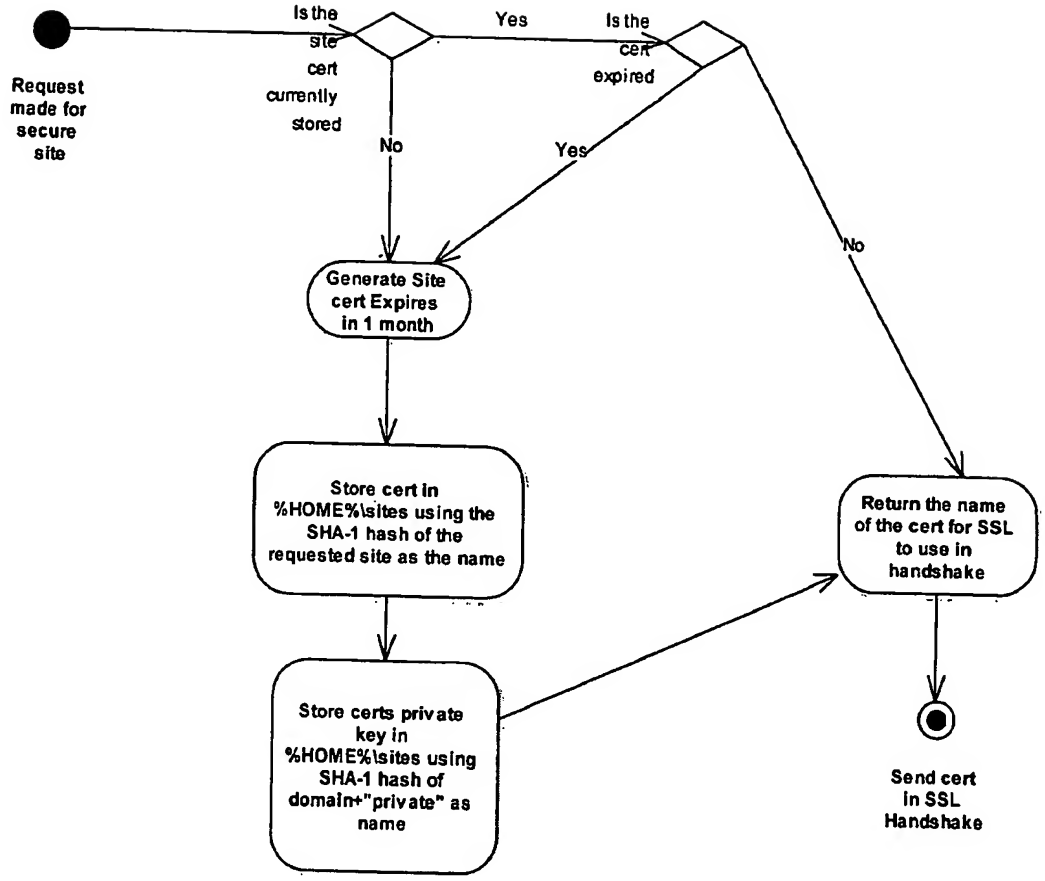
Request made for secure site
Is the site cert currently stored
Yes
Is the cert expired
No
Yes
No
Generate Site cert Expires in 1 month
Store cert in %HOME%\sites using the SHA-1 hash of the requested site as the name
Store certs private key in %HOME%\sites using SHA-1 hash of domain+"private" as name
Return the name of the cert for SSL to use in handshake
Send cert in SSL Handshake

FIG. 3

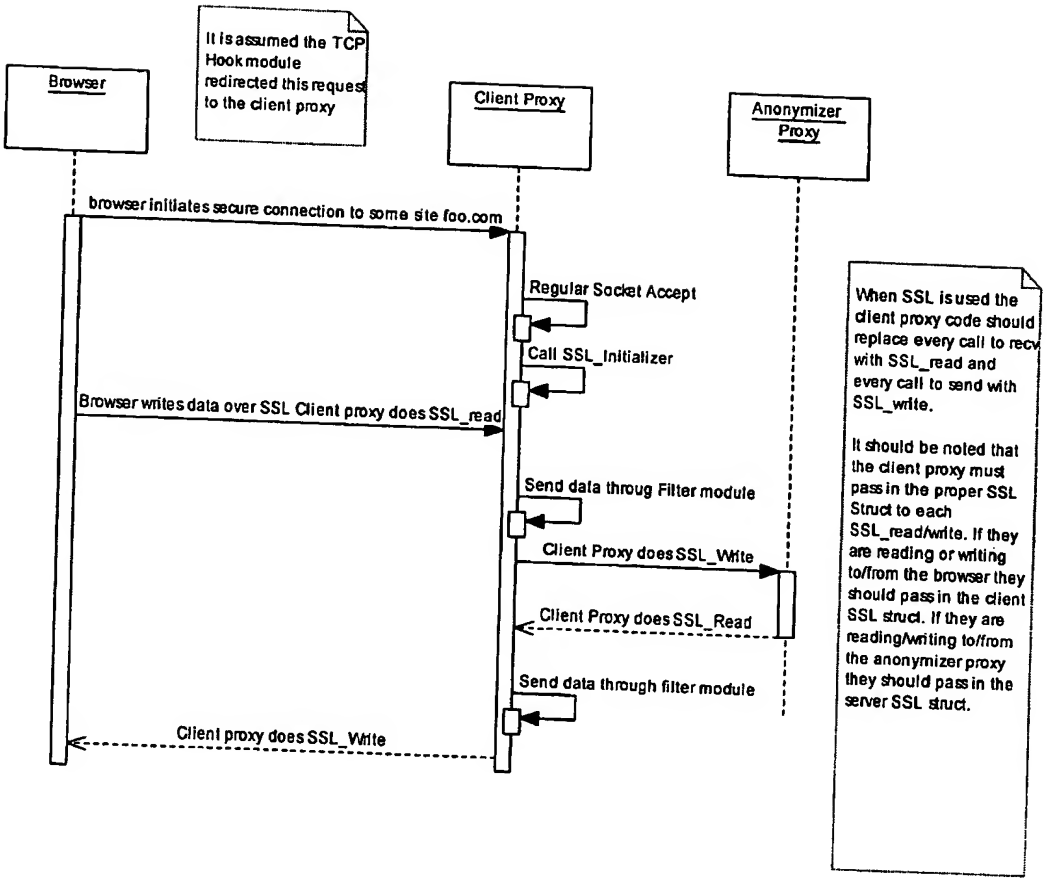
It is assumed the TCP Hook module redirected this request to the client proxy
Browser
Client Proxy
Anonymizer Proxy
browser initiates secure connection to some site foo.com
Regular Socket Accept
Call SSL_Initializer
Browser writes data over SSL Client proxy does SSL_read
Send data throug Filter module
Client Proxy does SSL_Write
Client Proxy does SSL_Read
Send data through filter module
Client proxy does SSL_Write
When SSL is used the client proxy code should replace every call to recv with SSL_read and every call to send with SSL_write.
It should be noted that the client proxy must pass in the proper SSL Struct to each SSL_read/write. If they are reading or writing to/from the browser they should pass in the client SSL struct. If they are reading/writing to/from the anonymizer proxy they should pass in the server SSL struct.

FIG. 4

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US04/020562

International filing date: 25 June 2004 (25.06.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/482,628
Filing date: 25 June 2003 (25.06.2003)

Date of receipt at the International Bureau: 02 September 2004 (02.09.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse